Method and apparatus for cryptographic communications using blind signatures

Publication number: EP0773647
Publication date: 1997-05-14
Inventor: CHAUM DAVID (US)
Applicant: SECURITY TECHN CORP (US)
Classification:
- international: ***G07F7/10; H04L9/32;*** *G06K7/00;* **G07F7/10; H04L9/32;** G06K7/00; (IPC1-7): H04L9/32
- european: G07F7/10D4E2; G07F7/10E; H04L9/32S1
Application number: EP19960203443 19890522
Priority number(s): EP19890913279 19890522; US19880198315 19880524

Also published as:
EP0773647 (A3)

Cited documents:
US4529870
XP000470378
XP000605075

Report a data error here

Abstract of **EP0773647**

A user controlled card computer C (110) and communicating tamper-resistant part T (120) are disclosed that conduct secure transactions with an external system S (130). All communication between T (120) and S (130) is moderated by C (110), who is able to prevent T (120) and S (130) from leaking any message or pre-arranged signals to each other. Additionally, S (130) can verify that T (120) is in immediate physical proximity. Even though S (130) receives public key digital signatures through C (110) that are checkable using public keys whose corresponding private keys are known only to a unique T (120), S (130) is unable to learn which transactions involve which T (120). It is also possible for S (130) to allow strictly limited messages to be communicated securely between S (130) and T (120). The user controlled card computer C (110) has: processing means (111); memory means (112); data entry means (113); data display means (114); and, two interfaces (125, 135). Tamper resistant part (120) has electromagnetic shielding (115).

Data supplied from the ***esp@cenet*** database - Worldwide